IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An apparatus to enable operation of a computer by authorized users when in a secure mode of operation, the apparatus comprising:

a hub, the hub being configured to be portable and in communication with the computer, the hub further including,

an installed system tray program configured to allow on demand customization of hub features using a graphical user interface;

a card reader,

a hub microprocessor, and

an encryption engine configured to encrypt/decrypt data communications between the hub and a data storage device protected by the hub, the encryption engine including,

a plurality of encryption/decryption channels, and

a control logic that is configured to determine which encryption/decryption channel is available and direct encrypted data passing through the hub to available encryption/decryption channels;

a card, the card being configured for insertion into the card reader, the card including a card microprocessor; and a user authentication device, the user authentication device being configured to validate the user as an authorized user of the card wherein, if the user is validated as the authorized user, the card microprocessor being configured to pass a key to the hub microprocessor in response to the validation of the user as the authorized user of the card, thereby activating the encryption engine of the hub to allow encryption/decryption of data communications.

2. (Original) The apparatus as recited in claim 1, wherein the hub includes a plurality of USB ports.

3. (Original) The apparatus as recited in claim 1, wherein the hub includes a plurality of FIREWIRE ports.

4. (Original) The apparatus as recited in claim 1, wherein the computer is connected to the hub through one of a USB or FIREWIRE interface.

5. (Original) The apparatus as recited in claim 1, wherein the user authentication device is a biometric scanner.

6. (Original) The apparatus as recited in claim 5, wherein the biometric scanner scans one of a fingerprint, an iris and a face.

7. (Original) The apparatus as recited in claim 1, wherein the card microprocessor includes a cryptographic microprocessor.

8. (Canceled)

9. (Original) The apparatus as recited in claim 1, wherein the hub includes control switches to bypass the hub to operate the computer in a non-secure mode of operation.

10. (Currently Amended) A computer security system for a computer, comprising:

a portable encryption control device, the encryption control device being in communication with the computer, the encryption control device including,

a card reader, the card reader being in communication with an encryption control device microprocessor,

a biometric identifier, and

an encryption engine configured to encrypt/decrypt data communications between the portable encryption control device and a data storage device protected by the hub, the encryption engine including,

a plurality of encryption/decryption channels, and

a control logic that is configured to determine which encryption/decryption channel is available and direct encrypted data passing through the hub to available encryption/decryption channels;

a system tray program configured to allow on demand customization of the portable encryption control device features using a graphical user interface; and

a card, the card being adapted to be read by the card reader to validate a user as an authorized owner of the card in conjunction with the biometric identifier, wherein upon validation of the user, the encryption engine activates to allow encryption/decryption of data communications.

11. (Canceled)

12. (Original) The apparatus as recited in claim 10, wherein the encryption engine executes RSA public-key cryptosystem.

13. (Previously presented) The apparatus as recited in claim 10, wherein the encryption control device is hot pluggable.

14. (Original) The apparatus as recited in claim 10, wherein the encryption engine is a field programmable gate array.

15. (Original) The apparatus as recited in claim 10, wherein the card includes a card microprocessor, the card microprocessor being configured to execute a challenge/response protocol for establishing a secure path through the encryption control device.

16. (Currently Amended) An apparatus for providing a secure operating environment for a computer, the apparatus comprising:

an encryption control device, the encryption control device (ECD) being in communication with the computer, the ECD further including,

an installed system tray program configured to allow on demand customization of the ECD features using a graphical user interface,

a card reader,

an ECD microprocessor,

an encryption engine configured to encrypt/decrypt data communications between the ECD and a data storage medium protected by the ECD, the encryption engine including,

a plurality of encryption/decryption channels, and

a control logic that is configured to determine which encryption/decryption channel is available and direct encrypted data passing through the ECD to available encryption/decryption channels, and

a biometric scanner;

a smart card, the smart card being configured for insertion into the card reader, the smart card including a smart card microprocessor, wherein upon the insertion of the smart card into the card reader, a secure path is established between the smart card microprocessor and the ECD microprocessor after completion of authentication of a user and completion of a challenge/response protocol, thereby unlocking the encryption engine to allow encryption/decryption of encrypted data communications.

17. (Previously presented) The apparatus as recited in claim 16, wherein the ECD includes the data storage medium.

18. (Previously presented) The apparatus as recited in claim 16, wherein the data storage medium is a virtual drive of the computer.

19. (Original) The apparatus as recited in claim 16, wherein the continued presence of a user is monitored.

20. (Original) The apparatus as recited in claim 16, wherein the ECD is locked by a hot key sequence.

21. (Previously presented) The apparatus as recited in claim 16, wherein the ECD is configured to effectuate modifying of encrypted data.

22. (Currently Amended) The apparatus as recited in claim 1, wherein the customization of hub feature[[s]] includes an ability to allow a user to select secure hub ports and permits a user to enable remote locking of the hub.

23. (New) The apparatus as recited in claim 10, wherein the customization of the portable encryption control device includes an ability to allow remote locking of the portable encryption control device.